Copia Real de Interfaces

Problema

De cara a realizar copias de trafico, en muchas ocasiones se recurre a la tecnología de port mirror, o su implementación de Cisco, SPAN (Switched port analyzer) o RSPAN (remote span). Esta tecnología nunca fue diseñada para realizar copias de trafico de manera estable, sino para tareas de troubleshooting
Realizar copias de trafico con mirror/span es simplemente imposible, ya que las comunicaciones en las líneas de comunicaciones son bidireccionales, y un port mirror no podrá nunca copiar una línea bidireccional de 1 Gb sobre una línea unidireccional de 1Gb.
Podríamos caer en la tentación de pensar que la línea no va totalmente llena, y que no tendremos problemas de sobresuscripción, pero cuando los picos de trafico de entrada mas salida superen la capacidad del interfaz, tiraremos trafico, lo que supondrá tirar todo la sesión cuando el equipo receptor sea statefull. En caso de ser una aplicación de seguridad, simplemente perder un paquete puede ser catastrófico

Por ultimo, si investigamos sobre las capacidades de nuestro fabricante de switching/routing, veremos que todos los fabricantes implementas medidas de protección a los equipos por los que si se supera cierto umbral de trafico en la línea de mirror, proceden a tirar el interfaz, de ara a no poner en riesgo la tarea principal del equipo

Solución

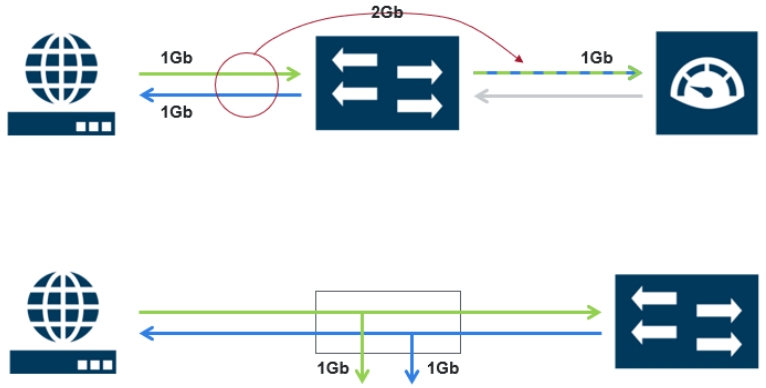
La única solución que realmente copia el trafico, y todo el trafico de un enlace, son los TAPs (Test Acces Port). Se trata de dispositivos que actúan a modo de "T": se intercalan en una línea de comunicaciones y sacan un replica exacta del trafico

De esta manera, una línea bidireccional de comunicaciones es convertida por el TAP en 2 líneas unidireccionales de la misma capacidad, por lo que se extrae la copia literal del trafico

Existen varios tipos de TAPs, en función del medio físico sobre el que se quiere sacar la copia del trafico:

- Pasivos (para interfaces de fibra): se trata de un equipo sin sistema operativo, alimentación ni SW que simplemente divide la luz entre la línea principal y la de copia. En realidad, es un simple prisma óptico
- Activos (para interfaces de cobre): equivalentes a los anteriores, pero requieren de alimentación para el propio interfaz de cobre
- Virtuales: de cara a capturar trafico en entornos virtuales, Gigamon dispone de SW capaz de extraer trafico en entornos AWS, Azure, GCP, VMWare (ESX/NSX/NSX-T), openstack, Nutanix, Kubernetes

Esquema



Licencias

TAPs
vTAPs

LINK